UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,460	08/04/2006	David Naccache	1032326-000404	5746

21839 7590 12/15/2010
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	
NOTIFICATION DATE	DELIVERY MODE
12/15/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
offserv@bipc.com

Office Action Summary	**Application No.** 10/588,460	**Applicant(s)** NACCACHE, DAVID	
	Examiner MICHAEL R. VAUGHAN	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16,18-21 and 23-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16, 18-21, and 23-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **8/30/10** has been entered.

Claims 17 and 22 are cancelled and claims 16, 18-21, 23-26, and 28 have been amended. Claims 16, 18-21, and 23-31 are pending.

Response to Amendment

Drawings

Claim Objections

Claim 31 was objected to for a minor informality. Even though claim 31 is not listed nor emphasized as being amended, it has in fact been amended to overcome the previous rejection as suggested by the Examiner.

Response to Arguments

Applicant's arguments filed 8/30/10 have been fully considered but they are not persuasive. The independent claims have been amended to include that the authentication medium **comprises** an electronic chip card. On page 2, of the arguments, Applicant states that claim 16 has been amended to recite that the authentication medium is an electronic chip card. As one can plainly see, the claim language does not support that narrow interpretation. Comprises broadly means includes. Thus the authentication medium could still be incorporated as some type of medium that just includes a chip card. Nevertheless for purposes of this argument Examiner will assume the claimed authentication medium is an electronic (IC) card.

Applicant alleges that the combination of Watanabe and Yamaguchi do not render the claims obvious. Specifically it is asserted that the combination does not disclose storing the encrypted biometric signature in the device to which the user requests access and transferring the encrypted biometric signature from the device to the electronic chip. Applicant purports this statement because he insists that Yamaguchi does not teach storing the encrypted biometric signature at the computer to which the user requests access. This point is moot because the primary reference, Watanabe, was relied up to teach this feature. Applicant is over complicating the combination in an attempt to render the 103 combination improper. However, taking the references as a whole, one of ordinary skill in the art would have known that storing the encrypted biometric data on the device and sending it to the IC for verification is within the ordinary capabilities of one of ordinary skill in the art because doing so produces a predictable result.

Turning to Watanabe, there are several embodiments which illustrate the scope of the invention. Figs. 24 and 27, for example, have been previously shown to teach the aspects of claim 16. Fig. 24 clearly shows the device, to which the user wants to access, stores the IDC (analogous to the claims encrypted biometric password). Fig. 27, another embodiment shows the user device sending just acquired biometric data to the IC where it is able to compare the stored IDC with the acquired biometric data. In this embodiment, the IDC is stored on the IC not the user device. It is for this reason a second reference was brought in to show why one of ordinary skill in the art might try to store the IDC in the user device instead of the IC card all the while still using the IC to perform the authentication. As both Watanabe and Yamaguchi teach, the IDC can be stored on the device or the IC (Yamaguchi fig. 42, and 0044). Regardless of the use of the access device it is still just one computer to which the user must authenticate to in order to gain any access into the system. There are two entities which can perform the authentication (IC card or device) and there are two places where the authenticated biometric data can be stored (IC card or the device). Therefore, four finite combinations are present and one of ordinary skill in the art could have tried any of them. Yamaguchi was also shown to teach why one of ordinary skill in the art might have chosen the combination present in the claimed invention. Since IC cards traditionally have limited memory, a computer device could store many encrypted biometric templates in a hard drive in a very efficient manner.

To summarize, Examiner finds Watanabe to teach storing the IDC in the user device. Watanabe also teaches performing the biometric matching in an IC card. Taking into account the teachings of Yamaguchi, it would have been obvious to combine the two embodiments of Watanabe, by simply storing the IDC in the user device, and sending it to the IC for authentication. This sending step inherently follows from the governing logic. Since it is beneficial to store the IDC on the user device and the user device is already sending the acquired biometric data to the IC for authentication, it must also send the IDC. In other words it is absolutely necessary to send the IDC to the IC because the IC is performing the authentication in this obvious arrangement. Just because Watanabe does not actually teach this embodiment does not mean one of ordinary skill in the art would not have tried this combination. With only four possible choices for arrangement, one of ordinary skill in the art could have tried any of them. As such a proper prima facie case of obviousness has been provided and therefore the 35 USC §103 rejection is maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 16, 18-21, and 23-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP Application Publication 2002/0069361 to Watanabe et al., hereinafter Watanabe in view of USP Application Publication 2001/0036301 to Yamaguchi et al., hereinafter Yamaguchi.

As per claim 16, Watanabe teaches a method of securing access to a piece of equipment, the method comprising:

obtaining a reference datum for an authorized user, in an authentication medium, wherein said reference datum comprises at least an encrypted authentic biometric signature [IDC] (0356);

storing an encrypted version of said authentic biometric signature on said piece of equipment (0335);

acquiring, at a sensor, a plain biometric signature for a user requesting access to said piece of equipment (0357);

decrypting, in said authentication medium, said encrypted authentic biometric signature (0356);

verifying, in said authentication medium, the authenticity of said plain biometric signature by comparing said plain biometric signature of said user with said decrypted authentic biometric signature of an authorized user (0357); and

granting said user access to said piece of equipment if said comparison is successful and denying access if said comparison fails (0357). While Watanabe teaches many embodiments of securing access to a piece of equipment, he is silent in explicitly disclosing a single embodiment teaching all of the above mentioned limitations combined with storing said encrypted authentic biometric signature on a piece of equipment and transmitted it to the authentication medium. Watanabe does teach storing the encrypted profile on computers in other embodiments. Moreover, Yamaguchi teaches that encrypted biometric templates are stored on a computer (see Figure 42 and paragraphs 0040 and 0044-46). Yamaguchi teaches hundreds of templates can be stored on a traditional computer database and hard drive. It is known that smart cards have limited memory. It is inherent that if the encrypted biometric sample is stored on the computer, and the IC card is performing the comparison, then the encrypted biometric sample must be sent to the IC card. In the cited Watanabe embodiment, the IC card obtains both the encrypted biometric sample and the input biometric sampling for authentication. The claim would have been obvious because combining known methods which produce similar results is within the capabilities of one of ordinary skill in the art. Watanabe teaches the encrypted biometric signature is decrypted in the smart card; the same result is achieved whether it was always stored there, or was retrieved from a computer database.

As per claim 21, Watanabe teaches a method of securing access to a piece of equipment, the method comprising:

creating a reference datum for an authorized user in an authentication medium comprising an electronic chip card, separate from said piece of equipment, wherein the creation of said reference datum (0198) comprises:

(i) inputting a personal identification code for said authorized user on a keyboard (0198 and 0248);

(ii) detecting, at a sensor, a plain authentic biometric signature for said authorized user (0198);

(iii) encrypting said plain authentic biometric signature by means of a private key (0198 and 0199);

(iv) sending said encrypted authentic biometric signature to said piece of equipment (0234);

(v) associating said personal identification code with said encrypted authentic biometric signature (0248); and

(vi) storing said encrypted authentic biometric signature and said associated personal identification code on said computer (0248);

receiving a personal identification code inputted on a keyboard (0248);

acquiring, at a sensor, a plain biometric signature of a user requesting access to said piece of equipment (0357); and

verifying the authenticity of said plain biometric signature for a user requesting access to said piece of equipment, wherein said verifying comprises:

(i) matching said personal identification code with an encrypted authentic biometric signature stored on said computer (0554);

(iii) decrypting said authentic biometric signature, on said authentication medium, by means of a private key on said authentication medium (0357);

(iv) comparing, on said authentication medium, said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result (0357); and

(v) granting access to said user requesting access to said piece of equipment if said comparison result is successful and denying access if said comparison result fails (0357).

While Watanabe teaches many embodiments of securing access to a piece of equipment, he is silent in explicitly disclosing a single embodiment teaching all of the above mentioned limitations combined with storing said encrypted authentic biometric signature on a piece of equipment and transmitted it to the authentication medium. Watanabe does teach storing the encrypted profile on computers in other embodiments. Moreover, Yamaguchi teaches that encrypted biometric templates are stored on a computer (see Figure 42 and paragraphs 0040 and 0044-46). Yamaguchi teaches hundreds of templates can be stored on a traditional computer database and hard drive. It is known that smart cards have limited memory. It is inherent that if the encrypted biometric sample is stored on the computer, and the IC card is performing the comparison, then the encrypted biometric sample must be sent to the IC card. In the cited Watanabe embodiment, the IC card obtains both the encrypted biometric sample and the input biometric sampling for authentication. The claim would have been obvious because combining known methods which produce similar results is within the capabilities of one of ordinary skill in the art. Watanabe teaches the encrypted biometric signature is decrypted in the smart card; the same result is achieved whether it was always stored there, or was retrieved from a computer database.

As per claims 18 and 23, Watanabe teaches said electronic card includes a decryption module (0356).

As per claims 19 and 24, Watanabe teaches said electronic card includes a comparison module, and said comparing is performed in said electronic card (0357).

As per claims 20 and 25, Watanabe teaches said electronic card further comprises an encryption module (0346 and 0352). Examiner supplies the same rationale as recited in the rejection of claim 16 to store the encrypted biometric signature on the computer.

As per claim 26, Watanabe teaches a device for securing access to a piece of equipment, comprising:

a storage device in said piece of equipment, for storing an encrypted authentic biometric signature (0336) and a corresponding personal identification code of an authorized user (0554);

a sensor for acquiring a plain biometric signature of a user requesting access to said piece of equipment (0357); and

an authentication medium comprising an electronic chip card (IC) having a controller, wherein said controller:

decrypts said authentic biometric signature by means of a secret key (0356);

compares said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result; and grants access to said user requesting access to said piece of equipment if said comparison is successful and denying access if said comparison fails (0357).

While Watanabe teaching many embodiments of securing access to a piece of equipment, he is silent in explicitly disclosing a single embodiment teaching all of the above mentioned limitations combined with receiving said encrypted authentic biometric signature from said storage device, associated with said personal identification code **in the authentication medium**. Watanabe does teach storing the encrypted profile on computers in other embodiments. Moreover, Yamaguchi teaches that encrypted biometric templates are stored on a computer associated with said piece of equipment (see Figure 42 and paragraphs 0040 and 0044-0046). Yamaguchi teaches hundreds of templates can be stored on a traditional computer database and hard drive. It is known that smart cards have limited memory. It is inherent that if the encrypted biometric sample is stored on the computer, and the IC card is performing the comparison, then the encrypted biometric sample must be sent to the IC card. In the cited Watanabe embodiment, the IC card obtains both the encrypted biometric sample and the input biometric sampling for authentication. The claim would have been obvious because combining known methods which produce similar results is within the capabilities of one of ordinary skill in the art. Watanabe teaches the encrypted biometric signature is decrypted in the smart card; the same result is achieved whether it was always stored there, or was retrieved from a computer database.

As per claim 27, Watanabe teaches at least one computer for storing a plurality of encrypted authentic biometric signatures and a corresponding plurality of personal identification codes for a corresponding plurality of authorized users [inherent this registration process applies to more than one user; 0234], wherein said at least one computer:

Watanabe does not explicitly teaches delivering an encrypted authentic biometric signature to said authentication medium when receiving an access request from a user, such that said authentication medium is capable of providing a plurality of users secure access to said piece of equipment. Examiner supplies the same rationale for combining the feature of storing the signatures in a computer until the access attempt as taught by Yamaguchi and recited in claim 26.

As per claim 28, Watanabe teaches said authentication medium is an electronic card having a memory storing a secret key that cannot be read from outside [smart cards are known for their protected memory].

As per claim 29, Watanabe teaches an encryption module that encrypts an authentic biometric signature supplied in plain form to said sensor and delivers said encrypted authentic biometric signature to said at least one computer, in response to an encryption command (0234). Examiner supplies the same rationale as recited in the rejection of claim 16 to store the encrypted biometric signature on the computer.

As per claim 30, Watanabe teaches said secret key is a private key having a matching public key, and wherein said encryption module is included in said at least one computer and uses said matching public key to encrypt authentic biometric signatures (0235).

As per claim 31, Watanabe teaches said piece of equipment includes an encryption module for encrypting an authentic biometric signature for storage in said piece of equipment (0228).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431